FAA National Software Conference
Obsolete Electronic Hardware

Guidance for Software Aspects of Replacing Obsolete Electronic Hardware in Aircraft Systems

Will Struck
FAA TAD ANM-111
will.struck@faa.gov

1

CAST Position Paper P-32

- Guidance is from Certification Authority Software Team (CAST) Position Paper P-32, *Guidance for Assuring the Software Aspects of Certification When Replacing Obsolete Electronic Parts Used in Airborne Systems and Equipment*
- P-32 Revision 2, Accepted and Closed by CAST at CAST Meeting 28 in January 2000

2

FAA National Software Conference
Obsolete Electronic Hardware

Presentation Overview

- CAST P-32 Content
- Paper's Approach
- Software Aspects
- Hardware Aspects
- System Considerations
- Summary

3

Related Regulations and Guidance

For Changes to Certified Aircraft Products:

- FAR 21.91-.101 (TC),
  21.115 (STC),
  21.611 (TSO)
- FAA Order 8110.4A, Type Certification Process, Section 14, Paragraph c., "Changed Aviation Products"

4

Additional Guidance

- FAA Notice N8110.85 and CAST Position Paper P-33, "Guidelines for the Oversight of Software Change Impact Analyses Used to Classify Software Changes as Major or Minor"
- Goals: achieve at least "an equivalent level of safety and confidence" in the modified product; and ensure software still functions correctly when replacing obsolete parts.

5

Paper 32 Content
High Level

- 1. INTRODUCTION TO SOFTWARE GUIDANCE FOR OBSOLETE ELECTRONIC PART REPLACEMENT
- 2. CAST POSITION
- 3. HARDWARE ASPECTS
- 4. SYSTEM CONSIDERATIONS
- 5. SUMMARY AND CONCLUSIONS

6

Paper 32 Content
Section 1

- 1. INTRODUCTION TO SOFTWARE GUIDANCE FOR OBSOLETE ELECTRONIC PART REPLACEMENT
- 1.1. PURPOSE
- 1.2. SCOPE
- 1.3. BACKGROUND
- 1.4. REFERENCES (14)

7

Paper 32 Content
Section 2

- 2. CAST POSITION
- 2.1. DETERMINING IMPACTS ON THE SOFTWARE
- 2.2. IMPACT CASES ON SOFTWARE
- 2.2.1. NO IMPACT ON SOFTWARE
- 2.2.2. PARTS REPLACEMENT WITH MINOR IMPACT ON SOFTWARE
- 2.2.3. PARTS REPLACEMENT WITH SIGNIFICANT IMPACT ON SOFTWARE
- 2.3. RESOLVING IMPACTS ON THE SOFTWARE
- 2.4. RE-ESTABLISHING THE SOFTWARE ASPECTS OF CERTIFICATION

8

FAA National Software Conference
Obsolete Electronic Hardware

Paper 32 Content
Section 3

- 3. HARDWARE ASPECTS
- 3.1. FORM, FIT AND FUNCTIONALLY INTERCHANGEABLE
- 3.2. PART REPLACEMENT WITH MINOR IMPACTS ON OTHER PARTS
- 3.3. PART REPLACEMENT THAT SIGNIFICANTLY IMPACTS OTHER PARTS

9

Paper 32 Content
Section 4

- **4. SYSTEM CONSIDERATIONS**
- **4.1. OBSOLETE ELECTRONIC PART SAFETY ASSESSMENT**
- **4.2. ASSESSING IMPACT ON SYSTEM FUNCTIONALITY AND PERFORMANCE**
- **4.3. ASSESSING IMPACT ON OPERATIONAL ASPECTS**
- **4.4. ENVIRONMENTAL QUALIFICATION / NON-INTERFERENCE**
- **4.5. SYSTEM ASSURANCE AND APPROVAL**

10

Paper's Approach

- Conduct change impact analysis to determine potential effects of new part on system aspects (including system reliability, performance and operational characteristics, and other systems), other system hardware components and software components; and perform regression testing to ensure no adverse effects of part's replacement.

11

Paper's Approach (Continued)

- If effect is none or insignificant, little effort and data is needed.
- If effect is significant, then various levels of effort and assurance will be needed, depending on system's criticality, architecture, software level(s), existing data and proliferation of effects.
- Coordinate plan with certification authority
- All effects should be re-verified (using regression testing) to ensure continued operational safety.

12

Software Aspects

- Identify impacts on software
- Identify specific software components and data affected; also significance of impact
- Determine software modification needed
- Determine plans for replacement and re-assuring software
- Coordinate with certification authority
- Implement plans and re-verify software
- Submit data as needed for software aspects

13

Software Aspects (continued)

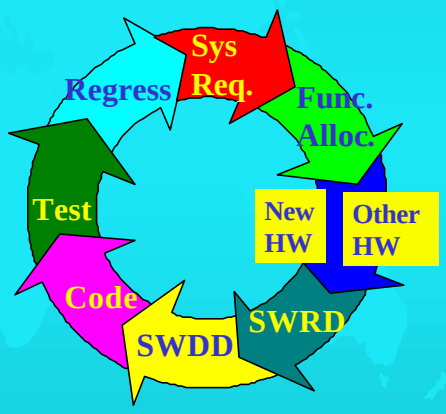
Types of Analyses to Determine the Impact:

- Traceability
- Data Coupling and Control Coupling
- Performance, Timing, Memory
- Input, Output, Interface, Bus Loading
- Partitioning/Protection/Isolation/Separation
- Redundancy, Safety Monitoring

14

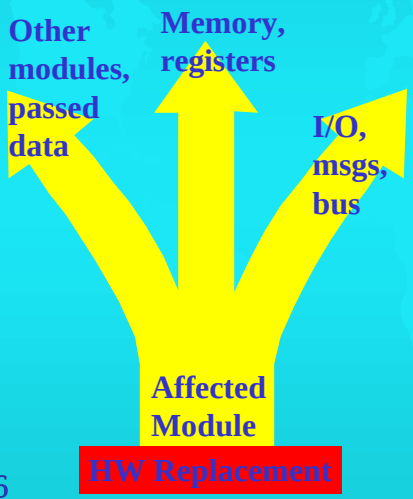
Traceability Analysis

- Identify affected:
  - System Requirements and Functions
  - Replaced HW and other HW Components
  - Software Requirements
  - SW Design Elements
  - Code
  - Tests and analyses to be performed to re-verify replacement



15

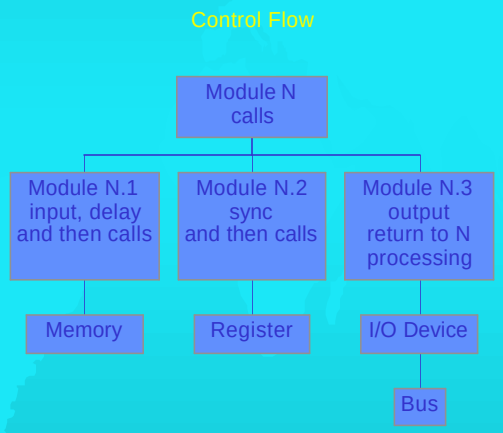
Data Coupling (Flow) Analysis



- Identify affected data coupling/flow with:
  - Other SW modules & parameters (passed data)
  - Memory, registers (shared data)
  - I/O devices, data msgs on bus (I/O data)
  - Data exchange sequence and timing

16

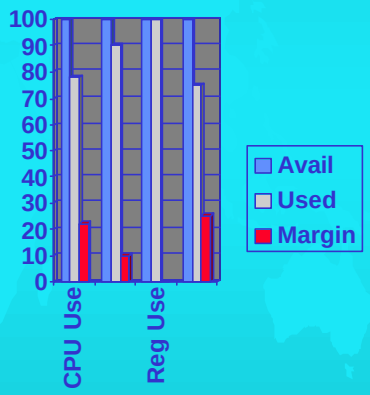
Control Coupling Analysis



17

Timing and Memory Analysis

- **Performance-Timing Usage of CPU, I/O devices, data buses, synchronization, timers, etc. (Timing Margin)**
- **Memory Usage of RAM, ROM, Cache, Registers, Buffers, etc. (Memory Margins)**



18

Safety Feature Analysis

- Ensure Partitioning (time and space), Protection Mechanisms (e.g., watchdog timer, sync), Isolation/Separation Means (independence) are maintained
- **Ensure Redundancy (e.g., comparators, cross-talk, voting logic, independence, etc.) mechanisms and integrity are preserved.**

19

Safety Feature Analysis (cont.)

- **Ensure Safety Monitoring (e.g., recovery means, independence of control and monitor functions, fail safe mechanisms, etc.) means and integrity are maintained.**
- **Ensure Resource Management (e.g., task scheduling, semaphores, contention resolution, timing, etc.) means and integrity are maintained.**

20

Replaced Device Functions

- **Ensure replaced device built-in functions (e.g., memory management, timers, registers, scheduling, instruction set, priority schemes, store/retrieve, etc.) are analyzed and verified for the replacement part.**

21

Software Aspects (continued)

Problem Areas:

- Non-existent software life cycle data
- Old, poorly documented software data
- Software design not consistent with code
- Software poorly controlled (CM) during life
- Spaghetti Code
- Traceability data not available

22

FAA National Software Conference
Obsolete Electronic Hardware

Hardware Aspects

- Basically the same process for hardware as for software
- Identify impact on other hardware components of the system
- Environmental qualification testing and non-interference demonstration may be needed.
- Allow for “family” parts and service history, if relevant

23

Hardware Problem Areas

- Less Mil-Std parts available; COTS hardware
- Unable to find/procure similar parts
- Incompatibility of electronic parts
- Unused functions in replacement parts
- Unintended and unknown side-effects of parts
- Problem history of replacement parts
- Combining formerly separate functions on single component (loss of independence and separation).

24

System Considerations

- Identify any impacts on aircraft or system safety, functional or performance requirements, operational or maintenance aspects, EQT/non-interference
- Coordinate with certification authority
- Verify & validate as needed
- Submit data for approval

25

FAR 21.93

- **Major change**
  - any change that has an appreciable "effect on weight, balance, structural strength, reliability, operational characteristics, or other characteristics affecting the airworthiness of the product."

26

System Problem Areas

Reliability

- **no service history (reliability numbers) for replacement part**
- **less durable parts (e.g., temperature extremes, vibration, salt spray, fungus, etc.)**

Operational Characteristics

- **Displayed information**
- **Human Factors**
- **Operating Procedures**
- **Maintenance/Repair**
- **Changed interfaces or data to other aircraft systems**

27

System Problem Areas

Other characteristics affecting airworthiness:

- **Incompatibilities with other aircraft systems**
- **HIRF, EMI, and Lightning Effects**
- **Aircraft maintenance schedules**
- **Replacement part integrity**
- **Operating procedures and training**

28

Other Considerations

- Simple versus Complex
- Criticality of system and "function" of obsolete part within the system and its architecture
- Certification process - "level playing field" and general policy needed.
- Compliance data submittals

29

Simple And Complex

- Simple devices can likely be readily tested and/or analyzed to determine impact and the lack of design errors.
- Complex devices cannot be readily verified and so must rely on design assurance, architecture mitigation, safety monitoring and other means of ensuring continued airworthiness

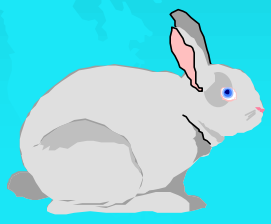
30

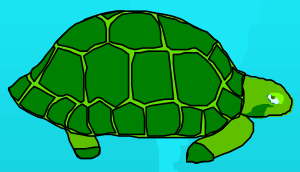
Criticality and Part's Role

- Less critical systems should need less effort, and more critical, more effort
- The use or function of the obsolete part and its potential failure conditions should have an effect on the level of effort
- If the system's architecture has mitigating means of reducing potential risks, less effort may be needed.

31

Level Playing Field





- The tortoise won but only because the hare got careless and lazy.
- Competitive advantages and disadvantages of a level and an un-level playing field
- Inconsistent application by ACOs

32

Clear, Standard Guidance

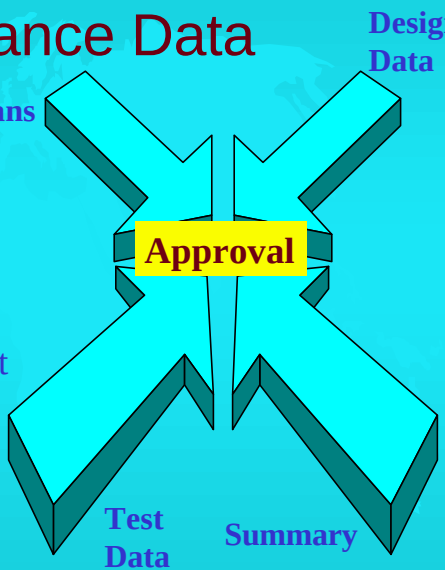
- Agreement on what should be done when replacing obsolete parts
- Standard Policy
- Training for industry and for certification authorities

33

Compliance Data

Dependent on:

- Major versus Minor
- System Criticality
- Part's Role in Arch.
- Significance of impact in terms of affected components and re-verification needed



34

Summary

- Obsolete part replacement should be fairly straightforward and standard - it's done all the time, though more of an issue now
- Policy for industry, certification authorities (engineers and inspectors), Flight Standards, and designees (DER, DMIR, DAS, ODA)
- Training and visibility of policy and how others have done and are doing it.

35

Questions?

36